opentext™

Security:

Creating Trust in a Zero Trust World

CEO White Paper

Mark J. Barrenechea
OpenText CEO and CTO

Contents

Introduction

At the dawn of the computer age, computers were not connected. Security was easy: put the computer in a room and set up physical security to make sure only authorized users enter the room. That was all there was to it.

When computers could be networked with a central system, security became more complicated. Still, protection was within reach. The idea of the physical perimeter became abstracted; the model of perimeter cybersecurity was born. A company's on-premises, enclosed network was its castle and perimeter security was the moat. Access controls permitted authorized users over the moat and into the castle. And within the castle, users were trusted to move freely.

With the advent of the internet, the perimeter became fuzzy. It was a new world of widespread networking, remote access and rapid information exchange. New technologies, like mobile devices and cloud, poked even more holes in the perimeter.

Today, cybersecurity is evolving again. The world is becoming increasingly connected and complex in the fourth industrial revolution. Cyberattacks are dynamic, difficult to predict and the stakes are higher. Cybercriminals have the latest technologies at their disposal. Machines are deployed against the enterprise's defenses, operating at a galactic scale, with volume, speed and agility humans can scarcely comprehend. Organizations need to counter machines with machines to have any hope of stymieing today's advanced threats. It is a machine versus machine world.

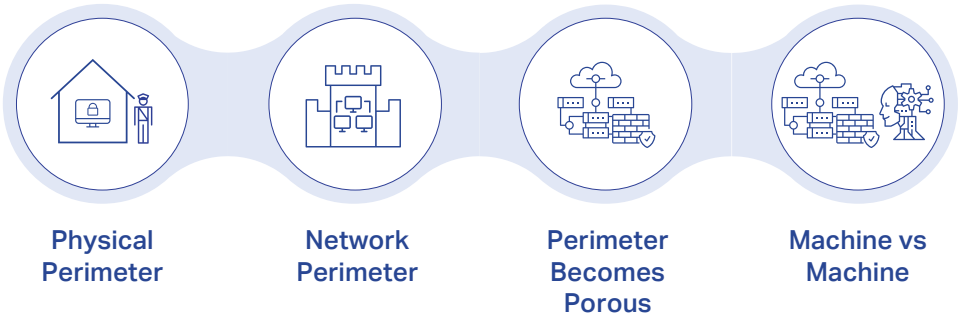


Figure 1:
A Simplified History of Cybersecurity

There is no place for 20th century security models in a 21st century network. Cybersecurity must evolve. The threat is growing—and so are the impacts.

The Growing Threat

Digital transformation has changed the world, spurring the rise of new technologies, new cultural paradigms and new business models. In this information age, data is constantly flowing into and out of the enterprise from every imaginable source. Endpoints are multiplying. Employees are working on-site, at home and in the coffee shop. Supply chains are global. Everything is connected.

Unfortunately, everything that is connected can be hacked. Large scale data breaches have become commonplace over the last decade. It is happening in every industry.

A global sportswear brand had 150 million accounts belonging to a subsidiary stolen in a data breach. The company's shares dropped almost 4%.[1] Meanwhile, direct losses of a huge data breach at a U.S. hotel group, in which half a billion customer records were compromised, climbed as high as $600 million.[2] On the heels of this breach, a question-and-answer site confirmed that its systems had been hacked. Weeks before, hackers accessed the personal details of 29 million accounts from a major social networking site.[3]

On October 2, 2019, the FBI issued a rare warning against high-impact ransomware attacks threatening U.S. organizations and businesses.[4] Ransomware (malware that takes control of a system or business network and holds it hostage until a ransom is paid) is becoming more targeted, sophisticated and costly. It threatens every organization, from governments to industrial companies, healthcare to the transportation sector. And everything in between.

Every day, another organization joins the club—those who have been hacked and those who are about to be.

Accenture and the Ponemon Institute have reinforced that cybercrime is "increasing, takes more time to resolve and is more expensive for organizations." In fact, after surveying hundreds of leading companies, they found that the average cost of cybercrime to organizations rose 12% last year to $13M.[5] Compared to mid-2018, the number of reported breaches was up 54%, and the number of exposed records was up 52%—setting up 2019 to be the "worst year on record."[6]

While cybersecurity itself is indeed complex, the underlying reason for this rise in breaches is simple: ever-growing risks combined with insufficient security practices.

Companies that experienced a breach of sensitive data within the last 12 months, up from 43% in 2015 (Forrester, 2019)

The average cost of a data breach in 2019, not including drops in share value (Ponemon Institute, 2019)

Data breaches caused by human error, not hacking (Shred-it Report, 2019)

Internet-enabled devices in use by 2025 (Strategy Analytics, 2019)

Increase in privacy class action lawsuits in 2020 (Forrester, 2019)

Figure 2:

Escalating Security Risks [7 8 9 10 11]

The attack surface grows with every passing day. Two-thirds of employees use their own devices for work, with some using more than one (think cell phone, tablet, personal laptop, wearable technology…).[12] This "bring your own device" (BYOD) trend is unstoppable and requires new security measures to manage these myriad endpoints.

Further, the endpoints may be on or off the business network. Either way, the enterprise is responsible for them. Today's technology users are digital nomads—they are mobile, virtual. Right now, every large organization has employees sitting in Starbucks and Dunkin' Donuts, working on open networks. You own that. Developers are opening virtual machines on AWS or Azure. You own that, too. The enterprise must protect business data from leaking to consumer applications, secure information on open networks, and maintain privacy and compliance. It must be able to determine whether any specific device can be trusted at any given time. It's your edge—secure it, protect it, isolate it, investigate it, defend it. Own it.

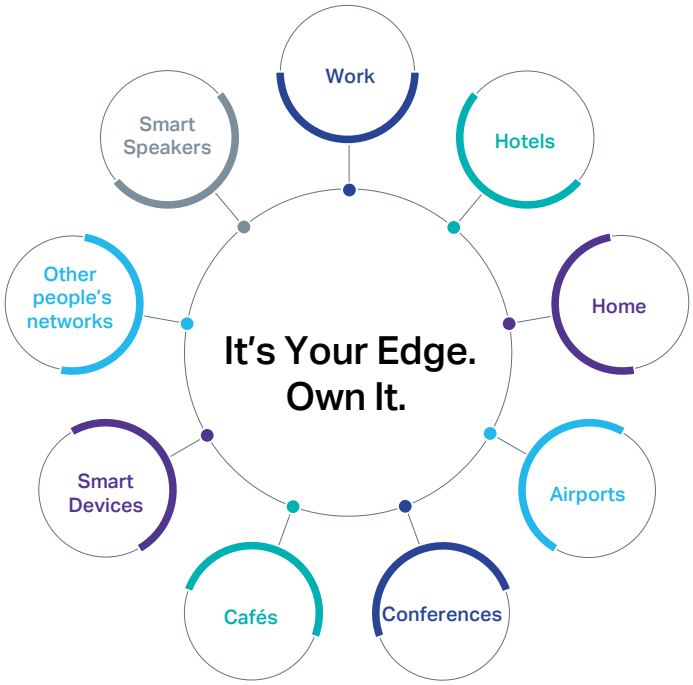


Figure 3:
It's Your Edge. Own it.

On top of BYOD, the Internet of Things (IoT) is creating billions of new endpoints and transmitting massive amounts of information. As the amount of data grows, so too do the opportunities for it to be compromised. If IoT devices are not adequately secured, they serve as ideal entry points to the rest of the network—especially when they are within a perimeter security model.

At the same time, regulations, security and governance are all converging around data requirements to comply with information privacy laws like the General Data Protection Regulation (GDPR) in Europe, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Children's Online Privacy Protection Act of 1998 (COPPA) in the U.S. To keep up with these regulatory pressures, the enterprise needs adaptable and defensible governance practices in place.

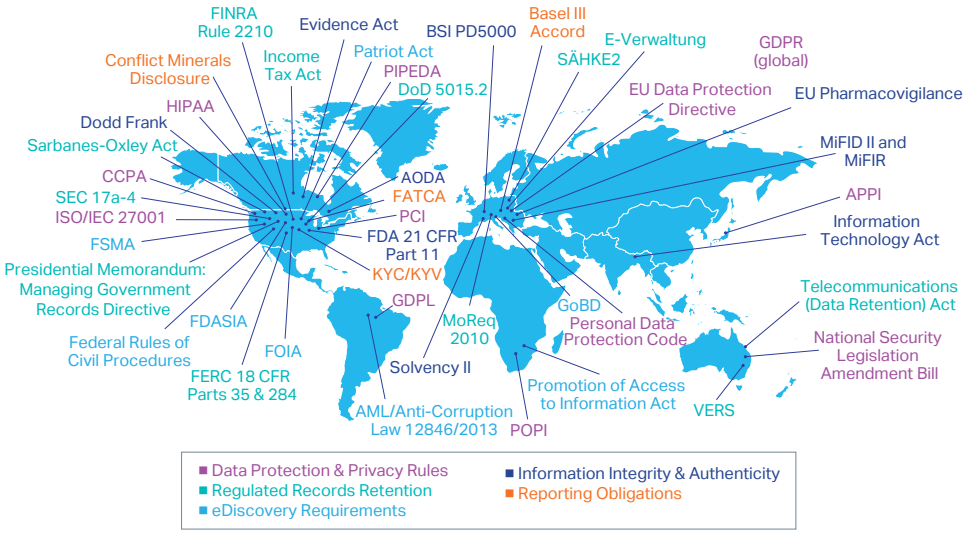


Figure 4:

Regulatory Pressures

The enterprise no longer exists in isolation. The days of contained, on-premises networks are long gone. Today's organizations operate on and off-cloud. As cloud computing becomes the norm, enterprise infrastructure becomes increasingly complex and distributed. Whether public, private or hybrid, cloud computing involves new kinds of application deployments, microservices, containerization and serverless functions. How do we secure a system that, by its very nature, we cannot put a wall (or even a decent fence) around?

The classic perimeter strategy trusts those already inside the network and assumes threats are external. Users are treated with "trust, but verify" policies, giving them broad access once they are deemed "trusted." Protection involves perimeters around all possible access points to the enterprise ecosystem, including networks, firewalls, VPNs, gateways, endpoints and data centers.

However, none of this helps when the bad actors are *already inside the network*. The average dwell time for threats in a corporate network is 100 days; the threat enters the system and waits over three months before acting.[13] Traditional security does not have the tools necessary to root out these lurkers before they can do harm. Add the fact that 53% of breaches are caused by simple human error from the enterprise's own employees, and it is clear that giving users free rein once inside the perimeter is a bad idea.[14]

Malicious insider threats—like disgruntled employees, corporate espionage or foreign government agents—must also be guarded against. Everything must be monitored for suspicious activity.

Traditional approaches also cannot effectively secure edges outside of the perimeter. Often, they cannot even determine how to handle BYOD devices *within* it. They are blind in the distributed cloud. And when a user account is compromised, cybercriminals can walk straight through the front door and gain access to everything.

The castle-and-moat approach to cybersecurity is dead. The castle no longer exists, rendering the moat moot. Vulnerabilities permeate all levels of business systems.

With more sophisticated hackers on the rise, new technologies and data formats, and a plethora of regulations, how will the enterprise manage all of its data, secure it and ensure that it is compliant?

Cybersecurity is in dire need of a reboot. Today's threats cannot be fought with yesterday's strategies.

The enterprise needs a new model of security: Zero Trust.

A Zero Trust Approach to Security

Zero Trust is a network security model based on the idea of "never trust, always verify." Users and endpoints are not trusted until they are authenticated—and even then, they only gain access to specific, limited applications and data. On top of that, they must reauthenticate periodically to maintain their access. Smart threat detection technologies patrol the network, analyzing patterns and flagging anomalous or suspicious behavior.

With holistic Enterprise Information Management (EIM) technologies, critical data is centralized and protected within layers upon layers of security extending from the heart of the enterprise out to all endpoints. Protection is complete against all attack vectors, external or internal.

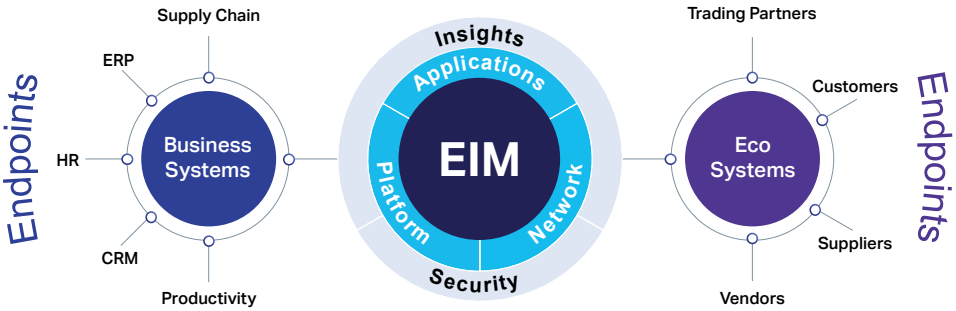


Figure 5:

EIM at the Center of the Enterprise

Zero Trust is strict and vigilant.

It starts with the basics:

1. Let's understand who the user is.
2. Let's understand the endpoint being used for access and its security status.
3. Let's enforce a conditional policy that specifies access.

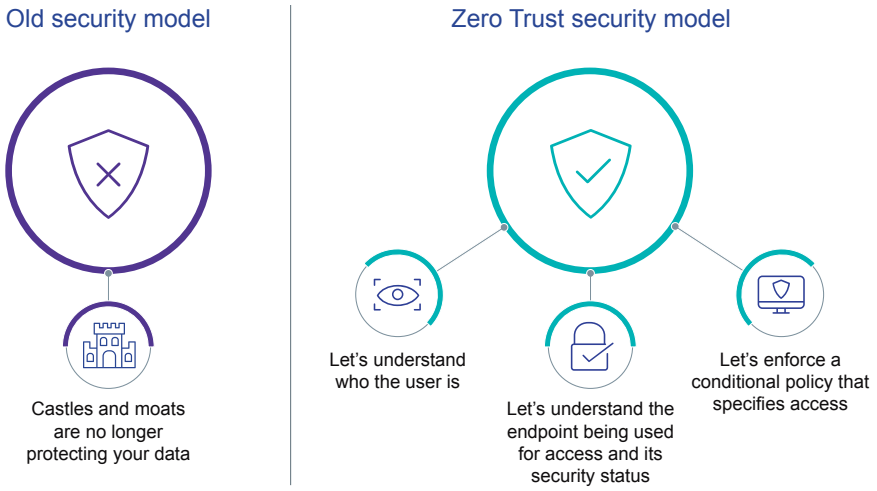


Figure 6:

Zero Trust Is the Effective Security Model

Understanding **who the user is** involves a technology foundational to the Zero Trust model: Identity and Access Management (IAM).

Before allowing access to company hardware and applications, IAM authenticates and authorizes each user. An IAM system includes automated lifecycle management for both internal and external users, comprehensive identity governance, privileged access management and integrated multi-factor authentication (MFA) capabilities. It stops identity sprawl to third parties, centralizing and protecting identities.

However, securing identities is just the beginning. One of the most common ways bad actors circumvent enterprise security protocols is through endpoints. All edges are vulnerable—servers (both on-premises and on-cloud), workstations, desktops, laptops, tablets, mobile devices. That is why a Zero Trust security system must **understand every unique endpoint and its security status**. It must have complete visibility and control over any endpoint requesting access.

In a security landscape where business users (and their endpoints) have become hyper-mobile, employees are digital nomads working from various geographies and types of locations. Certain places carry higher risks. Endpoint security applications help organizations to keep pace with this new way to work by integrating with the enterprise Virtual Private Network (VPN) and micro-segmenting to keep endpoints protected, regardless of where they are. Remember: own your edge.

Micro-segmentation underpins successful endpoint security, and indeed, the entire Zero Trust security approach. It calls for enterprises to segment based on users, their locations, the sensitivity of data and other categories. Once this is done, organizations gain granular visibility into traffic and can enforce multiple layers of monitoring, inspection and access control based on the "who, what, where, when, why and how" of devices and users attempting to access the protected surface. This is known as "Layer 7" policy—and it is what makes Zero Trust security possible. Nothing gets in or out without rigorous vetting.

With micro-segmentation, the entire threat vector changes. No one can get everything. Proper separation prevents most data from even being in the crosshairs of hackers. The only way bad actors can get to it is individually, which is difficult because they would have to first identify each individual entry point. Further, threat detection technologies are vigilant within this framework, watching for unusual behavior from any source, at any level.

But if (or when) bad actors do succeed, the targeted endpoint is equipped with endpoint detection and remediation technology that swiftly isolates, remediates and cleanses the threat.

In knowing exactly who each user is and the status of each endpoint, Zero Trust technologies make it possible for the enterprise to effectively **enforce conditional access policies**—also known as "least privilege access"—to restrict each user's access to only the resources they need. No more, no less.

This is done using IAM protocols, which allow the Zero Trust enterprise to set role-based and attribute-based access controls (RBAC and ABAC). Different levels of security and access are applied to different types of accounts and users. Even the most privileged users, like those with administrative privileges, are subject to access controls.

Least privilege lowers the risk of unintentional or malicious data leaks, either by internal users or attackers using stolen credentials. As with micro-segmentation, no one can get everything.

To enforce least privilege/conditional access policies and effectively micro-segment, the enterprise needs to assess its data and data management policies in detail. Data must be classified based on considerations like role access, risk tolerance, data sensitivity and regulatory requirements.

Questions to ask in this exercise include: What data is sensitive to my organization? Where is this sensitive data located? What devices possess sensitive data and how can we keep a closer watch on them? Is there a system in place to alert the security team when sensitive data changes locations? Who needs to have access to this data? Are unauthorized users accessing this restricted data or storing it where it should not be stored?

Segmenting like this also helps companies comply with increasing regulations for issues like data privacy and data retention.

Assessing which obligations apply to the enterprise is a serious undertaking, given the complexity of evolving industry, regional, and international regulations as well as the harms of non-compliance. The costs of non-compliance (litigation, fines, stock drops, loss of customer trust, etc.) far outweigh the costs of putting the necessary policies, technologies and staff in place to ensure proper security and governance. This is true across the board, but especially for industries like financial services, healthcare and general government sectors that handle large quantities of sensitive data—a prime target for cybercriminals.

As the amount of data collected has skyrocketed, so have laws about data retention and disposal. Zero Trust helps the enterprise identify which data can be deleted and when, according to regulations for the defensible disposition of electronic data. Deleting data that the organization is no longer obligated to retain also reduces the volume of data that is vulnerable to attack. Less data means less risk.

Because perimeter-focused security policies have failed to protect enterprise data, security professionals are losing the battle of protecting their networks, devices, apps and people. The mindset of Zero Trust is data-centric "defense in depth." It solves cybersecurity problems by following the *data*, no matter where it travels.

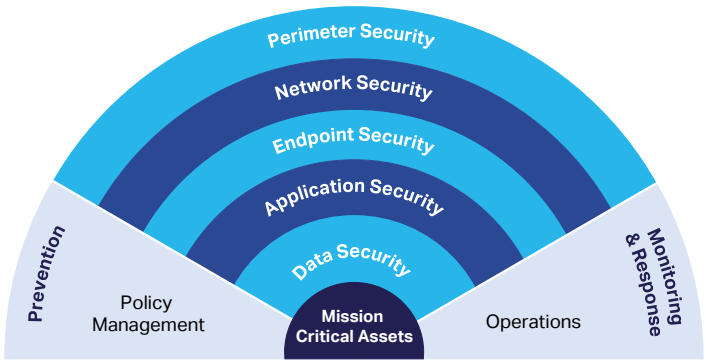


Figure 7:

Defense in Depth

Fortunately, as enterprises weave cloud into their technology stack, Zero Trust infrastructure becomes easier to deploy. Cloud has better visibility on endpoints, traffic, users and data than legacy infrastructure. It also scales and updates more easily, lending itself to micro-segmentation.

As with anything worth doing, implementing Zero Trust poses challenges.

Obstacles to Implementing Zero Trust

Although a Zero Trust approach is becoming necessary to combat growing cybersecurity threats, transitioning is not always easy for the enterprise.

Overcoming Legacy Systems and Technical Debt

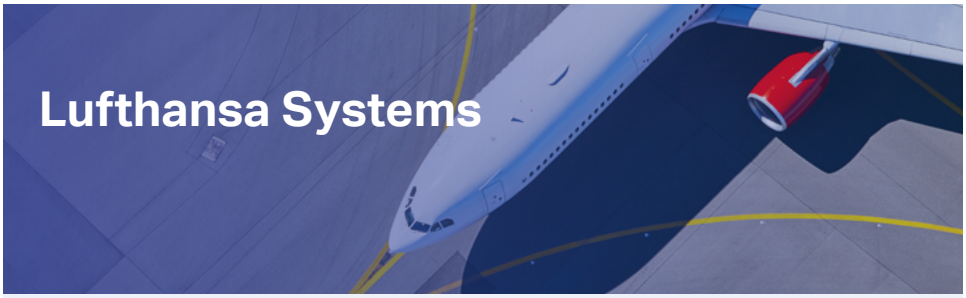
Most enterprise technology environments carry the burden of legacy applications, networks and protocols that were not built with agility or today's needs in mind. Reworking these systems takes significant effort, resources and investment—and typically the older they are, the more of this "technical debt" they have accrued.

Looking specifically at cybersecurity needs, most legacy enterprise applications have no concept of least privilege. For example, many legacy authentication models provide single sign-on, which falls short of the Zero Trust standard. They cannot layer with other technologies, like IAM or endpoint security.

As another example, peer-to-peer (P2P) technologies popularized in the late 1990s also tend to operate counter to Zero Trust. In Windows 10—used by most enterprise workforces—P2P can allow unauthorized lateral movement that can expose sensitive data, unless Windows Update sharing is turned off.

Mesh network technology relies on P2P communications, making it another potential weak spot. Its trust model is based on keys or passwords; it does not have the ability for dynamic Zero Trust authentication. As the latest breaches have made clear, protecting user access to enterprise environments with keys or passwords alone is doomed to fail. It is too easy for bad actors to get past these protocols and gain unlimited access.

Overcoming these legacy challenges requires investment in new technologies and a technology partner that can help create and deploy a true Zero Trust strategy.



Leading airline IT provider Lufthansa Systems, a subsidiary of Lufthansa, is one of the world's leading providers of IT services in the airline industry. They deliver innovative IT products and services to more than 350 customers worldwide. With growing demand for air travel, limited airspace capacity and ever-increasing costs, optimizing flight operations is a critical priority for airlines today. In response, Lufthansa Systems designed the Lido portfolio of flight planning solutions, pilot solutions and data solutions to help airlines improve operations. These products provide integrated optimization in real time for flight dispatchers and crews, from flight planning and execution to flight completion, while enhancing the safety of every flight.

Recently, the organization needed to replace its client access system for the roughly 4,000 users at 110 airlines who need to securely and reliably access the Lido applications. With focus on operational stability, they needed the migration from their legacy system to be seamless, so that it would not impact users.

As a result, Lufthansa Systems selected OpenText Exceed TurboX for centralized administration, robust security and solution stability. Exceed TurboX has delivered important benefits behind the scenes at Lufthansa Systems, including robust security, solution stability and valuable administrative abilities. In addition, Exceed TurboX provides strong security on several levels to protect the system from internal and external attacks. Keeping core applications in a central data center ensures there is no unauthorized access and strong encryption is used for the data traffic between the client browser and the Exceed TurboX web server, as well as for the screen content stream between a node and the client.

Endpoint Explosion and the Internet of Things

The attack surface has grown, largely because of the rapid surge in endpoints and the IoT. IoT is a major consideration for industries that already use a huge number of connected devices in their daily environments, as well as industries where this change is imminent.

Healthcare is one such industry, with over 100 million IoT devices around the world.[15] In the U.S., every hospital bed has 10 to 15 connected devices; yet, hospitals have lost track of about 30% of their devices, leaving them open to cyberattack.[16]

With so many endpoints to consider, migrating to Zero Trust can be daunting. But this large attack surface is precisely why these environments *must* be secured with Zero Trust technologies.

Enterprises tackling endpoint explosion can look to the cloud as a Zero Trust ally. Critical data can be taken off the endpoint and put in the cloud. Bad actors cannot get information from the endpoint if it is not there to begin with. Connecting to the cloud can also replace connecting to headquarters (e.g. for remote employees), providing better protection and visibility into traffic. Through cloud, Zero Trust can be enforced without inserting a firewall in front of every resource. This approach simplifies the architecture and reduces the opportunity for attack. And don't overlook the value of a Layer 7 solution, which enables administrators to understand and control the who/what/where/when/why/how of access to a cloud environment.

Regulatory Compliance

Industry regulations create more obstacles for Zero Trust deployment.

Privacy, retention and enterprise data governance regulations lay down limits on how data flows, how it is shared and how it should be protected. New requirements are constantly emerging as legislators and other stakeholders struggle to keep pace with the latest fourth industrial revolution trends and technologies—and the enterprise must keep up too.

One major example is the General Data Protection Regulation (GDPR) of 2016. Any corporation doing business in the EU or that has EU persons' data in its possession needs to comply with stringent GDPR privacy requirements—like disclosing privacy breaches to impacted individuals within 72 hours of identifying the breach, a turnaround time that many organizations struggle with. Non-compliance with the GDPR results in heavy fines.

The Health Information Portability and Accountability Act (HIPAA) is another important regulation, which applies to organizations doing business in the U.S. The healthcare industry collects a lot of sensitive personal data about nearly everyone, making it a big target for cybercriminals. HIPAA outlines restrictions on the use and disclosure of health information, to maintain high data privacy and safety standards across the industry. Every healthcare organization must have a dedicated privacy official responsible for adhering to HIPAA in collaboration with the Chief Information Security Officer (CISO) and legal counsel.

OCHIN

OCHIN, one of the largest, most successful health information networks in the United States, supports more than 500 organizations and 10,000 clinicians who serve more than 37 million patients nationwide. OCHIN's members use fax as part of their regular patient information exchange process, especially for services that haven't yet caught up with common electronic health record (EHR) data-sharing technology or are on an external system.

Fax system inefficiencies, health information security concerns and rising costs resulted in organizational challenges and didn't reflect the best standards in patient care. To address these challenges, OCHIN sought a secure, centralized fax solution that would integrate with its existing EHR. As a result, they decided to deploy OpenText™ RightFax™, a centralized fax server solution for powerful, secure and compliant faxing capabilities across an entire health organization. As a result of this deployment, OCHIN and its member clinics have seen improved operational performance, enhanced productivity and security, reduced costs and increased integration. By automating the exchange of fax information directly into the EHR, RightFax accelerated the flow of information to health care providers on OCHIN's system.

The financial industry is also a top target for cybercriminals. The Payment Card Industry Data Security Standard (PCI DSS) addresses the protection of credit cardholder data. The requirements are applicable to all system entities and components involved in Cardholder Data Environment (CDE)—that is, users, process workflows, and network or system devices that store, process and transmit cardholder or authentication data. Given the complexities of the PCI DSS, the enterprise needs to enlist its legal, information security, IT, risk, and operations teams to make sure that all angles are covered.

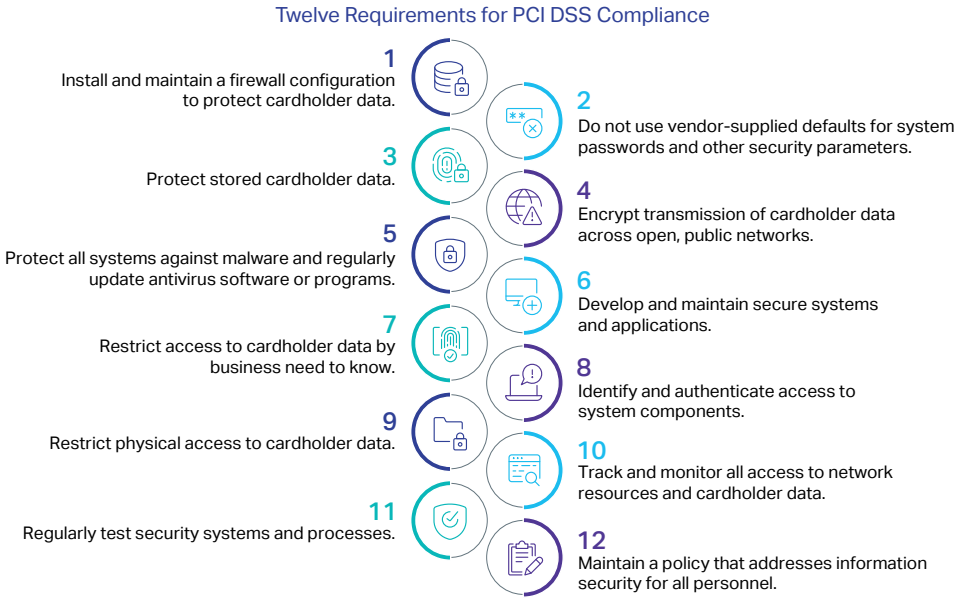


Figure 8:

PCI DSS Requirements

These are just a few of the regulations to be aware of when conducting business in today's digital economy. Each industry, region and country has its own set of regulations and standards that must be followed.

And it is not only your company that must be compliant. Businesses working with non-compliant third parties can be liable for damages along with the at-fault company. To protect the enterprise and its customers, every third-party vendor's privacy, risk and compliance programs must also be vetted.

The enterprise needs technologies that enforce governance and regulatory compliance policies from end-to-end and that can be updated as new standards emerge.

Such technologies protect the enterprise before an issue arises, falling under the category of proactive Zero Trust technologies.

Proactive Security Technologies

In the Zero Trust model, nothing is more important than proactively safeguarding enterprise data. Fortunately, many technologies exist to do just this.

Zero Trust technologies must work closely together to offer full coverage from threats. While they can be broken out individually, a true Zero Trust solution requires an intricate web of protection, arranged strategically for the enterprise's unique needs across all attack vectors.

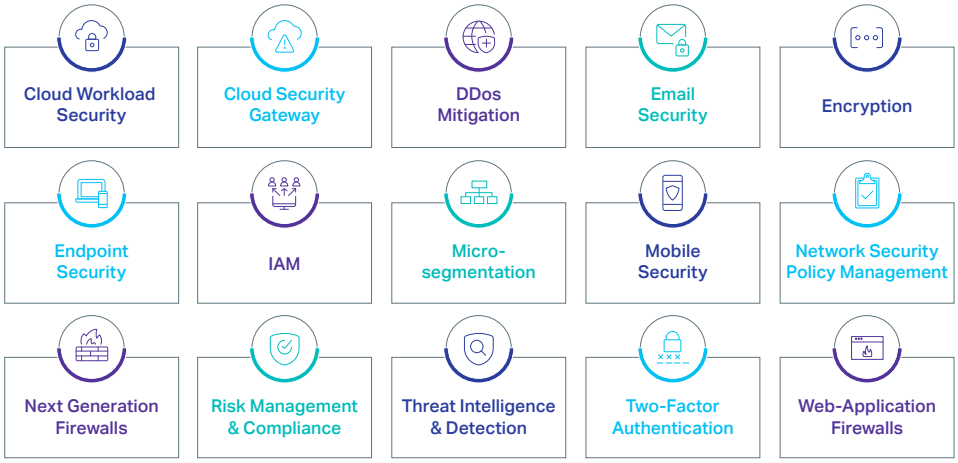


Figure 9:

Top Security Technologies—Proactive

Cloud Workload Security

Cloud workload security technologies protect workload execution in Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) environments. These solutions provide automated and layered controls to secure the configurations, network, applications and storage of hybrid cloud hypervisors and workloads.

Cloud Security Gateway

This technology provides visibility into how data moves to and from cloud services. It also enforces usage policies to cloud traffic and data by applying a proxy. Cloud security gateways reduce operational and investment costs while increasing business agility.

DDoS Mitigation

A distributed denial-of-service (DDoS) attack overwhelms a targeted system by flooding it with traffic and requests from multiple sources, making it unresponsive to its intended users. This type of cyberattack is carried out by machines or "bots."

DDoS mitigation solutions drop the bad traffic before it affects end user experience. For industries that rely on significant revenue from ecommerce or online transactions, DDoS mitigation technologies are essential. They ensure customer-facing sites and applications are resilient and protect revenue-generating transactions.

Email Security Technologies

This is particularly important because of the trend to migrate from self-managed on-premises email to cloud email, such as Office 365. Email security technologies generally include anti-spam, anti-phishing, anti-malware (including ransomware), data leak prevention and encryption techniques. These solutions also monitor outbound email traffic to thwart data loss and encrypt sensitive data.

Encryption

Encryption is a must. It is one of the most effective implementations of data security to prevent theft and protect privacy. Through a secret key known only to the intended recipient, encryption renders data unreadable to unauthorized parties.

Endpoint Security

Endpoint security solutions protect endpoint devices like laptops, mobile phones, IoT devices and servers. Deploying endpoint security is one of the most practical ways to enforce Zero Trust measures—including least privilege policies, user access control, and location and traffic monitoring.

Endpoint detection and response (EDR) is an important subset of endpoint security that should be implemented on all enterprise endpoints to monitor for threats. Once a threat is detected, this technology alerts the cyber security team, isolates the endpoint and remediates it, returning the IT environment to a trusted state. EDR is the last line of defense against digital theft. It focuses on uncovering and remediating issues before they escalate into more intrusive data breaches.

This approach to protecting endpoints eases the burden on the security team to track, detect and respond to threats. By alerting the team to the most relevant and critical security information first, and automating manual and repetitive tasks, security teams can use their resources where it matters most.

Identity and Access Management (IAM)

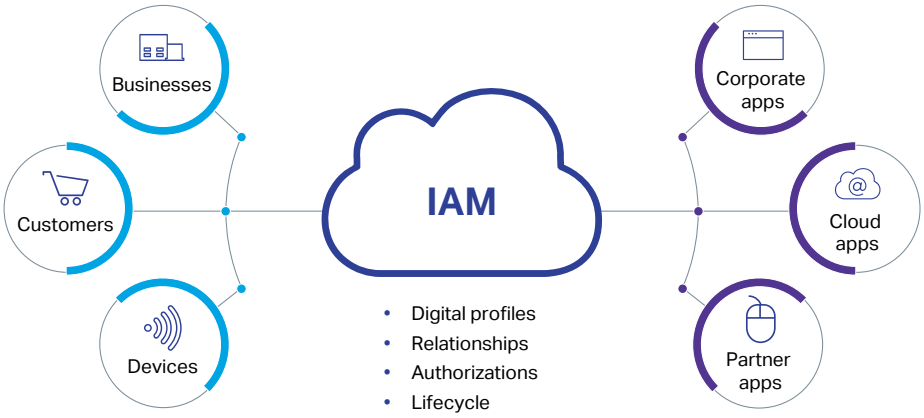


Figure 10:

Everything Needs an Identity

IAM manages all digital identities that request access to enterprise systems and applications, a key principle of Zero Trust. It centralizes and automates the governance of the identity lifecycle. And by increasing transparency and limiting access to sensitive data and apps, security teams can prevent incidents (or, limit the damage caused by them).

IAM technology is comprehensive. It provides role management and access governance to enforce least privilege, identity administration self-service, separation of duties, remediation, access request management, and compliance and audit support.

The Auto Club Group (ACG) – the second largest AAA club in North America – has selected OpenText to support a unified identity and access management solution for their 9 million members.

Using the OpenText Covisint platform, ACG can create a single digital member identity across all business units to reduce complexity, increase security, and streamline the digital experience for customers. OpenText Covisint provides the leading IoT and identity platform for digital business transformation. Working with ACG to create a single digital member identity will support ACG's strategic digital program objectives, including improving the overall user experience for the organization's AAA customers.

As organizations embrace digital transformation, identity and access management becomes essential for connected experiences. By securely connecting ecosystems of people, systems and things, companies like ACG can enable new service offerings, optimize operations, develop new business models, and ultimately, enable the connected economy.

Micro-segmentation

Micro-segmentation solutions subdivide networks into secure enclaves where granular security can be applied to data based on its sensitivity and value. This technology prevents attackers and insiders from moving across data centers and cloud deployments, limiting the impact of a breach to only the compromised segment.

Micro-segmentation is essential for an identity- and data-centric Zero Trust security model.

Mobile Security Suites

Mobile is here to stay. To keep environments secure, the enterprise must defend against mobile threats such as jailbroken devices, vulnerable software and sensitive data that could be traveling through unencrypted channels.

Mobile security applications protect devices, data and apps, making it easier for the enterprise to manage mobile holistically. They also increase visibility and help enforce compliance with corporate policies.

Network Security Policy Management

Most network device configurations have old, unnecessary and sometimes conflicting rules that impede device performance and provide bad actors with attack avenues. Network security policy management technology tackles this problem by automating network device configuration tasks, keeping everything up to date as security teams add new rules to support business processes.

Next Generation Firewalls

These multi-purpose security solutions replace standalone appliances for firewalls, intrusion prevention systems (IPS) and other security controls. With a hardware-based approach, they create micro-perimeters in Zero Trust network architecture design. By combining core security technologies with other functionalities into a single solution, next generation firewalls significantly simplify network architecture and management, along with reducing the cost of managing multiple security appliances.

Risk Management and Compliance Software

The amount of data stored by the enterprise has exploded exponentially, with new data constantly introduced. This data must be classified and tracked, for both compliance and security purposes.

Records, data governance and data remediation technologies are therefore among the top proactive measures that organizations can take. Risk management and compliance software is designed specifically to identify, classify and remediate sensitive data across the enterprise. It allows the enterprise to repeatably and defensibly manage the data lifecycle from collection to disposition.

Threat Intelligence and Detection Software

To sniff out external attack attempts, lurking bad actors and insider threats, threat intelligence and detection software analyzes behavior in real time. This software can stop an attack before it happens by flagging suspicious activity, blocking malicious inbound traffic and phishing attempts, and staying ahead of the latest malware. When the software finds an issue, the Zero Trust security environment can be immediately hardened against the threat.

Figure 11:

Monitoring Insider Threats

Two-Factor Authentication

Because passwords are not secure enough in today's cybersecurity landscape, two-factor authentication is a must-have. Offering substantially stronger protection than passwords alone, it should be used to safeguard critical data and applications, prevent data breaches and ensure audit compliance.

Some of the options for two-factor authentication include: physical biometrics (finger, face and voice), behavioral biometrics, software and hardware tokens, push notifications, one-time passwords (OTPs) and certificate-based authentication.

Web-Application Firewalls

A web-application firewall detects and blocks attack attempts from web applications. Applying security policies based on attack signatures, protocol standards and anomaly detection, it protects against basic bots, DDoS, Layer 7 attacks and data leakage. This technology can also satisfy regulatory compliance requirements, provide layered protection and defend zero-day vulnerabilities (weaknesses that have been found but not yet patched) until the environment can be strengthened against them.

Mastercard

Mastercard, a technology leader in global payment industry, has partnered with OpenText to help companies increase financial efficiencies across global supply chains, starting in the automotive industry. Given that B2B has become a huge priority for the company as it looks to expand services beyond credit cards, Mastercard realized that payments is just one piece of the puzzle. There is often a patchwork of processes and lack of interoperability in the whole B2B space which results in a lack of trust within the auto industry ecosystem.

The new solution from OpenText and Mastercard will streamline many of the operations processes while providing peace of mind to business buyers. The goal is to increase the speed, compliance and security for business information, payments and financing in the automotive supply chain. It is designed to facilitate integrated payments and to enhance the management of vendor master data, enabling suppliers to better manage risk for trade finance, accelerate cash flow for outstanding invoices and secure financial transactions with enhanced digital identity. This collaboration further advances a connected and scalable digital ecosystem, allowing companies, irrespective of size, location or technical capability, to build increased trust and security into trading partner relationships.

As threats mount and enterprise environments become increasingly complex, proactive security technologies are converging onto holistic security platforms—most notably, on Endpoint Protection Platforms (EPP)—to ensure unified protection at a level impossible for distributed and federated systems. EPPs are emerging that integrate the most vital Zero Trust technologies, including anti-malware, exploitation prevention, detection, isolation, remediation and behavioral threat detection.

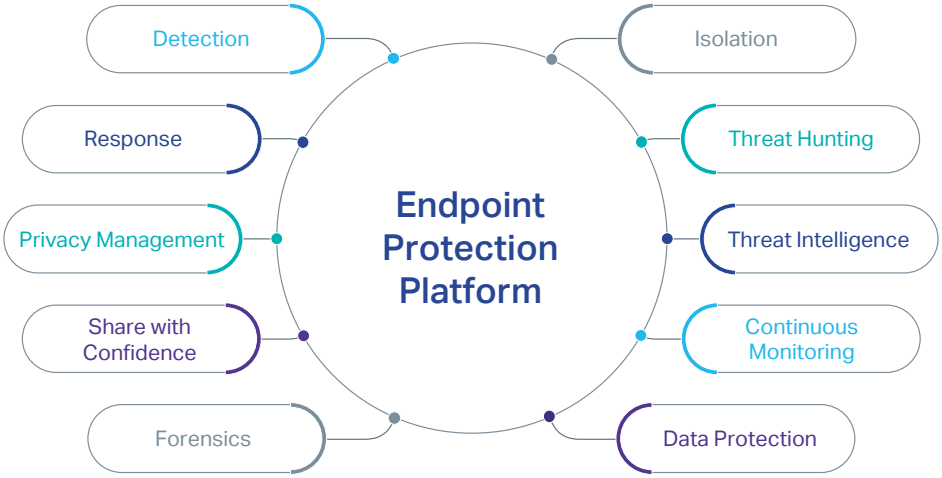


Figure 12:

An Integrated Zero Trust Security Platform

An ounce of prevention is worth a pound of cure—but it is still wise to have the cure at hand. Likewise, the enterprise needs to be ready to respond to breaches if (and when) they occur.

Reactive Security Technologies

Even in a Zero Trust environment, organizations should have strong reactive security technologies. No matter how fortified a business is, new methods of breaking through cybersecurity are concocted every single day. It is like playing whack-a-mole: cybercrime constantly rears its ugly head and sometimes it breaks through. When that happens, organizations need to act fast. Decisively.

In the event of an intrusion, the enterprise needs technologies that can quickly isolate the compromised data sources, execute all legal hold notice policies, and begin the forensic examination process to measure the depth and breadth of the breach.

Figure 13:

Top Security Technologies—Reactive

Digital Forensics and Investigation

Digital forensics software allows for discreet, off-the-network and forensically-sound collection. It enables investigation, whether litigation, internal or in response to an administrative proceeding.

To protect its value as evidence, organizations need to follow forensic investigatory best practices when collecting data, like avoiding altering the data, documenting everything, making forensic copies of all digital evidence as quickly as possible, and only reviewing the evidence via these forensic copies. Whether working with a third-party forensic expert or using internal resources, these precautions will lead to the best outcomes as well as minimize allegations that evidence has been withheld, destroyed or altered (aka spoliation claim).

Figure 14:

Digital Forensics

Technologies evolve quickly. Cloud, virtual networks, BYOD, social media applications, IoT, artificial intelligence… the list goes on. On top of this technological quagmire, add the vast and growing amount of digital information. All of this complicates the identification of relevant evidence, and the process of preservation and forensic investigation. Investigators must have the tools to cover all devices and operating systems, reach all data, and work discreetly and globally while ensuring a fast, efficient, repeatable and forensically-sound investigative process.

When assessing which security technologies to acquire, organizations should consider software and hardware that will address the broadest array of applications and scenarios within the business. The enterprise needs court-proven forensic collection tools built with the investigator in mind. It needs to reduce the window between incident detection and remediation. It needs to be holistic, going both deep and wide to protect the enterprise's most valuable assets.

Banner Health

Banner Health is one of the largest nonprofit healthcare systems in the U.S., with close to 500 medical facilities across six states, including hospitals, urgent care facilities and rehabilitation centers. In a single year, Banner Health sees more than a million emergency room visits, runs close to five million blood tests and delivers more than 30,000 babies.

With both cybersecurity threats and litigation on the rise, Banner Health determined its existing systems could not meet the company's increasingly critical needs and sought other methods to accelerate data security response. To support the organization's commitment to patient care, Banner Health made the decision to employ OpenText EnCase eDiscovery and OpenText EnCase Endpoint Investigator.

This helped to accelerate their eDiscovery processes and data security by providing the organization with a 360-degree visibility across all endpoints, devices and networks to enable forensically sound data collection for litigation. The automated EnCase eDiscovery solution allows the company to collect and preserve potentially relevant data from multiple data sources, with a process that ensures strict chain of custody and executes legal hold in a defensible manner. In addition, EnCase Endpoint Investigator collects and analyzes data for incident response and investigation. When a security alert is received, the solution's advanced digital forensic tools collects relevant data to quickly assess the situation and respond accordingly. Automating and accelerating many time-consuming processes, such as information collection, has enabled Banner Health to significantly improve its efficiency across all fronts.

eDiscovery

Once the forensic collection process is complete, all potentially-relevant data must be reviewed to find the answers to critical questions, such as: How did the breach occur? What endpoints were compromised? What enterprise data was targeted and/or stolen? Were data privacy laws violated, and if so, what notice requirements are triggered by this breach?

This is the eDiscovery phase, and it broadly covers the data processing, document review and analysis, and production stages.

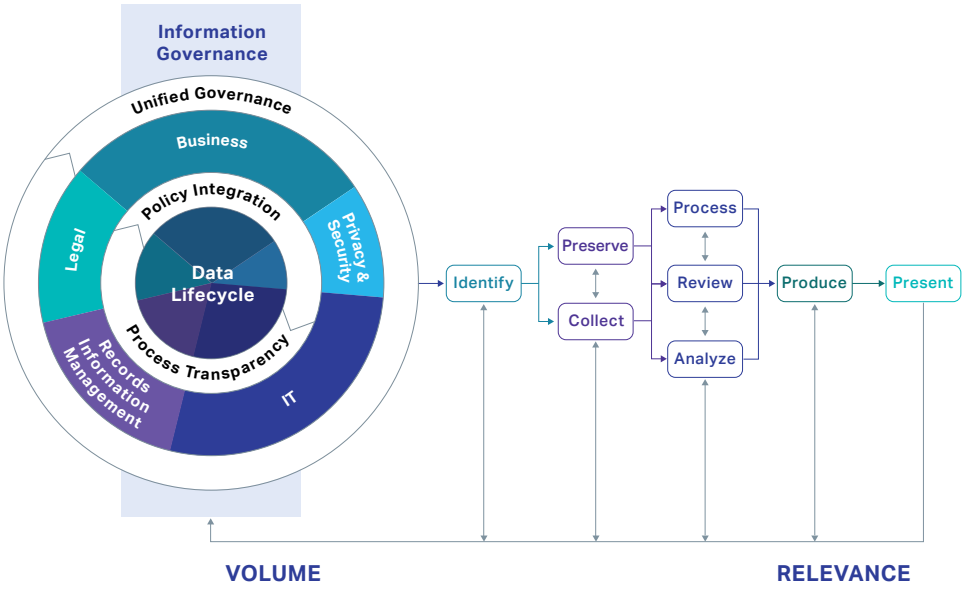


Figure 15:

Electronic Discovery Reference Model[17]

The goal is to determine, out of all the data collected during forensics, what must be produced to investigators (internal, external, law enforcement or administrative) or opposing counsel as a result of a breach. The process includes a data reduction step where the data population is reduced by date range, key custodians and keyword search terms into a smaller set of potentially-relevant information (most often emails, e-documents, etc.).

The best eDiscovery technologies include AI-driven analytics and automation that can help to intelligently extract, organize and narrow down the huge volume of documents to just those that are meaningful. This data is then put into a document review application so that legal teams, both internal and external, can easily review it.

Serious Fraud Office

The Serious Fraud Office (SFO) leads the UK's fight against serious and complex fraud, bribery, and corruption. Its investigations cross international borders, involve multi-million-pound (GBP) losses and huge volumes of data and correspondence across all document types to determine if criminal activity has taken place.

The SFO uses OpenText Axcelerate and OpenText EnCase to achieve next-generation, forensically-sound, AI-driven investigations. OpenText's visualized data analytics and predictive coding help the SFO's multi-disciplinary case teams tackle exponentially growing data volumes by automating key aspects of document analysis, enabling them to expedite investigations efficiently with limited resources. The SFO is leading the way in the use of digital technology for criminal investigations and considers OpenText their most important technology partner moving forward.

The enterprise needs a good defense *and* a good offense in the war against cybercrime. Especially when the battlefield is changing all the time.

The Only Constant Is Change

Cybersecurity will never stand still. As technology becomes more sophisticated, so do threats. Risk escalates in lock-step with the amount of data that needs to be protected—and today we are creating more information than we ever have before. And, less than we ever will again. The attack surface is growing and changing every day.

Consumers have already embraced the cloud, using it to store data about their entire lives—including their most sensitive personal information. Businesses, although slower to adjust, are also adopting the cloud en masse. Ninety-four percent of enterprises use at least one cloud service, and within a year, 83% of all enterprise workloads will be in the cloud.[18] While the cloud has disrupted traditional cybersecurity, it has great ability to enable Zero Trust security in the information era.

Only in the cloud can big data and analytics be leveraged over huge networks of endpoints to predict and manage threats in real time. Only the cloud can be updated effortlessly and automatically with the latest security upgrades, keeping it a step ahead. The more pervasive cloud becomes, the better it can mobilize to confront threats as soon as they are discovered. Consider an extensive cloud infrastructure that predicts a threat, isolates it before it can do any harm, then immediately updates itself to protect every customer organization against similar threats. This will be completely automatic, happening with the speed and scale required to compete in an environment of machines versus machines.

Data is moving fast (and faster still) within the cloud, through machine-to-machine (M2M) communications and between endpoints. 5G is coming and it will bring with it a wave of new devices that will be able to transmit and receive information with unprecedented density, speed and efficiency. 4G was designed for humans; 5G is designed for machines. At today's 22 billion devices, we are only seeing the beginning of the Internet of Things. By 2025, that number will almost double to 41.6 billion.[19 20] The IoT and 5G will dramatically shift the world's infrastructure to connect everyone and everything. The impact on the cybersecurity landscape will be enormous.

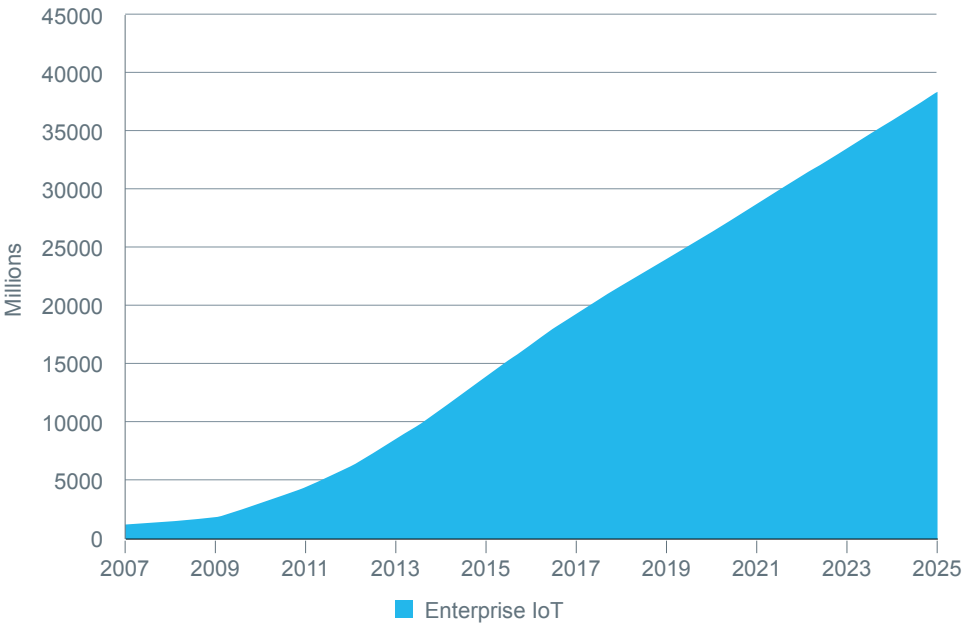


Figure 16:

IoT Will Change the World within Five Years

With 5G speed and the sheer volume of connected devices in the IoT, it is obvious that both legacy systems and human oversight will be (and already are) utterly inadequate. Machine-speed attacks are increasing and cannot be stopped with human-dependent defenses. Enter: artificial intelligence. AI and machine learning can analyze big data from across the enterprise in real time, recognize patterns, make predictions and automatically respond to deviations and threats. Businesses are taking note. Eighty-three percent of organizations in the U.S. believe that they will not be able to stop cyberattacks without AI.[21] As machine learning becomes more integrated in cybersecurity defenses, it will become smarter and smarter in identifying and responding to threats.

Moving further into the future, the impact of quantum computing cannot be overstated. Quantum will change the game yet again. Today's encryption standards—2048-bit RSA encryption—would take the world's current computing power, working together, millions of years to break. In all practicality, this encryption is currently unbreakable. However, quantum computing operates according to different rules. In about 25 years, there will be a quantum computer that can break the encryption in only *eight hours*.[22] What does this mean for cybersecurity? We will need new information security standards using post-quantum codes that cannot be cracked by quantum computers.

Cybersecurity will continue to evolve with the technology. To handle tomorrow's threats, security technologies are becoming integrated, converging on solutions like Endpoint Protection Platforms. The enterprise cannot afford to let its security infrastructure lag behind.

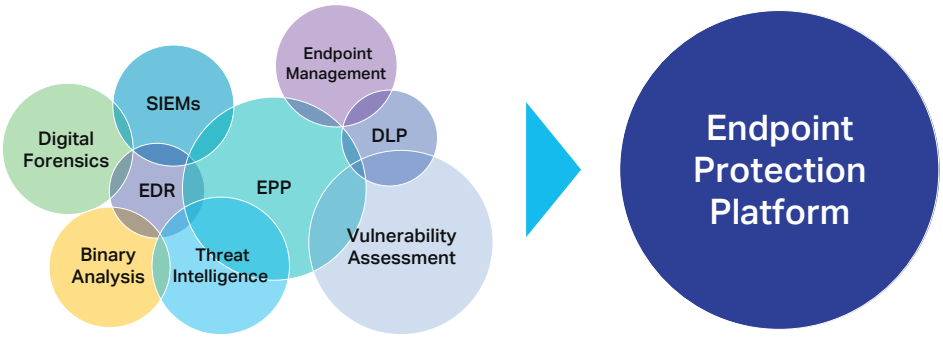


Figure 17:

Converged Security Platform

Consider the adage: "You can't step in the same river twice." The Zero Trust cybersecurity environment is like a river—with a constant ebb and flow of new threats, changing data formats, evolving compliance requirements and emerging technologies altering the ecosystem with every passing moment. There will never be a point in time when we can say: "That's it. Our information is secure. We are done."

Organizations need to act. They can protect themselves by staying current and choosing technology partners with best-in-class holistic security solutions. To succeed, change must be embraced. That means taking cybersecurity seriously and committing to continuous improvement. It means being proactive. It means fighting machines with machines. It means implementing a Zero Trust infrastructure. It means jettisoning old ways of thinking.

Zero Trust security is not just a new set of policies and technology deployments. It is a new paradigm for approaching the protection and governance of the enterprise's most valuable asset—information.

Endnotes

[1]Nick Statt, *"Under Armour says 150 million MyFitnessPal accounts compromised in data breach,"* The Verge, March 29, 2018, *https://www.theverge.com/2018/3/29/17177848/under-armour-myfitnesspal-data-breach-150-million-accounts-security* (accessed November 2019).

[2]Judy Greenwald, *"Direct cyber incident losses from Marriott breach up to $600M: AIR,"* Business Insurance, December 18, 2018, *https://www.businessinsurance.com/article/20181218/NEWS06/912325732/Direct-cyber-incident-losses-from-Marriott-breach-up-to-$600-million-AIR-Worldwi* (accessed November 2019).

[3]Russel Brandom, *"Facebook hacker accessed personal details for 29 million accounts,"* The Verge, October 12, 2018, *https://www.theverge.com/2018/10/12/17968302/facebook-hacker-personal-details-29-million-accounts* (accessed November 2019).

[4]Davey Winder, *"FBI Issues 'High-Impact' Cyber Attack Warning—What You Need To Know,"* Forbes, October 3, 2019, *https://www.forbes.com/sites/daveywinder/2019/10/03/fbi-issues-high-impact-cyber-attack-warningwhat-you-need-to-know/#79bb2fea40af* (accessed November 2019).

[5]Kelly Bissell, Ryan M. Lasalle and Paolo Dal Cin, *"Ninth Annual Cost of Cybercrime Study,"* Accenture, March 6, 2019, *https://www.accenture.com/us-en/insights/security/cost-cybercrime-study* (accessed November 2019).

[6]Samantha Ann Schwartz, *"Data breaches up 54% YOY, 2019 set to be 'worst year on record',"* CIO Dive, August 21, 2019, *https://www.ciodive.com/news/data-breaches-up-54-yoy-2019-set-to-be-worst-year-on-record/561359/* (accessed November 2019).

[7]Jennifer Adams, *"Security Outlook 2019: Modest Growth, But Some Sectors Will See Double-Digit Increases,"* Forrester, June 18, 2019.

[8]Larry Ponemon, *"What's New in the 2019 Cost of a Data Breach Report,"* Security Intelligence, July 23, 2019, *https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/* (accessed November 2019).

[9]Meera Narendra, *"Human error remains the main cause of data breaches,"* PrivSec Report, June 20, 2019, *https://gdpr.report/news/2019/06/20/human-error-remains-the-cause-of-data-breaches/* (accessed November 2019).

[10]*"Strategy Analytics: Internet of Things Now Numbers 22 Billion Devices But Where Is The Revenue?"* Strategy Analytics, May 16, 2019, *https://news.strategyanalytics.com/press-release/iot-ecosystem/strategy-analytics-internet-things-now-numbers-22-billion-devices-where* (accessed November 2019).

[11]Fatemeh Khatibloo, Heidi Shey, Enza Iannopollo and Stephanie Liu, *"Predictions 2020: Privacy And Data Ethics,"* Forrester, October 30, 2019.

[12]Deyan G., *"41 Stunning BYOD Stats and Facts to Know in 2019,"* TechJury, April 17, 2019, *https://techjury.net/stats-about/byod/* (accessed November 2019).

[13]Chase Snyder, *"What Is Dwell Time in Cyber Security?"* ExtraHop, May 21, 2019, *https://www.extrahop.com/company/blog/2017/dwell-time-new-security-metric/* (accessed November 2019).

[14]Meera Narendra, *"Human error remains the main cause of data breaches,"* PrivSec Report, June 20, 2019, *https://gdpr.report/news/2019/06/20/human-error-remains-the-cause-of-data-breaches/* (accessed November 2019).

[15]Statista Research Department, *"Estimated healthcare IoT device installations worldwide from 2015 to 2020,"* Statista, May 26, 2016, *https://www.statista.com/statistics/735810/healthcare-iot-installations-global-estimate/* (accessed November 2019).

[16]Zeljka Zorz, *"Healthcare's blind spot: Unmanaged IoT and medical devices,"* Help Net Security, July 22, 2019, *https://www.helpnetsecurity.com/2019/07/22/healthcare-iot/* (accessed November 2019).

[17]*"EDRM Model,"* EDRM, *https://www.edrm.net/resources/frameworks-and-standards/edrm-model/* (accessed November 2019).

[18]*"Cloud Adoption Statistics for 2019,"* HostingTribunal.com, *https://hostingtribunal.com/blog/cloud-adoption-statistics/* (accessed November 2019).

[19]*"Strategy Analytics: Internet of Things Now Numbers 22 Billion Devices But Where Is The Revenue?"* Strategy Analytics, May 16, 2019, *https://news.strategyanalytics.com/press-release/iot-ecosystem/strategy-analytics-internet-things-now-numbers-22-billion-devices-where* (accessed November 2019).

[20]*"The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast,"* IDC, June 18, 2019, *https://www.idc.com/getdoc.jsp?containerId=prUS45213219* (accessed November 2019).

[21]Ron Tolido, Anne-Laure Thieullent, Geert van der Linden, et al., *"Reinventing Cybersecurity with Artificial Intelligence,"* Capgemini Research Institute, July 2019, *https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf* (accessed November 2019).

[22]*"How a quantum computer could break 2048-bit RSA encryption in 8 hours,"* MIT Technology Review, May 30, 2019, *https://www.technologyreview.com/s/613596/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/* (accessed November 2019).

OpenText Locations

AMERICAS

Canada:
- Ontario - Ottawa
- Ontario - Richmond Hill
- Ontario - Waterloo
- Quebec - Montreal

USA:
- Arizona - Scottsdale
- Arizona - Tucson
- California - Irvine
- California - Pleasanton
- California - San Mateo
- California - Santa Barbara
- Colorado - Denver
- Florida - Tallahassee
- Florida - Tampa
- Georgia - Alpharetta
- Kansas - Overland Park
- Kentucky - Lexington
- Maryland - Gaithersburg
- Massachusetts - Boston
- Michigan - Southfield
- New Jersey - Tinton Falls
- New York - Latham
- New York - New York
- New York - Rochester
- Ohio - Hilliard
- Tennessee - Brentwood
- Texas - Austin
- Texas - Dallas
- Texas - San Antonio
- Utah - Draper
- Virginia - Arlington
- Washington - Seattle

Brazil:
- São Paulo

Mexico:
- Mexico City

EMEA

Austria:
- Klagenfurt
- Wien

Czech Republic:
- Prague

Finland:
- Helsinki
- Tampere

France:
- Paris

Germany:
- Düsseldorf
- Frankfurt
- Hamburg
- Hannover
- Hürth-Efferen
- Kempten
- Konstanz
- Munich (Grasbrunn)
- Oldenburg
- Rheinbach

Ireland:
- Cork

Italy:
- Rome, IT

Netherlands:
- Amstelveen
- Hoofddorp
- Putten
- Rotterdam

Poland:
- Poznań

Russia:
- Moscow
- St. Petersburg

South Africa:
- Johannesburg

Spain:
- Barcelona
- Madrid

Sweden:
- Gothenburg
- Stockholm

Switzerland:
- Baden

United Arab Emirates:
- Dubai, UAE

United Kingdom:
- London
- Preston
- Reading
- St. Albans

APJ

Australia:
- Melbourne
- Sydney

Greater China:
- Beijing
- Guangzhou
- Hong Kong
- Shanghai

India:
- Bangalore
- Hyderabad
- New Delhi

Japan:
- Tokyo
- Osaka
- Nagoya

Korea:
- Seoul

Malaysia:
- Kuala Lumpur

New Zealand:
- Wellington

Philippines:
- Manila

Singapore:
- Singapore

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit opentext.com.

Contact

Sales
Email: sales@opentext.com

Partners
Email: partners@opentext.com

Media Relations
Email: publicrelations@opentext.com

opentext.com/contact